CLAIMS

1. An information recording device for recording the information on a recording medium, comprising:

memory means for holding a node key unique to each node of a hierarchical tree structure having a plural number of such information recording devices, operating as leaves, and a leaf key unique to each information recording device, said memory means also holding a key renewal block formed as renewal key storage data decryptable using at least one of the node key and the leaf key; and

encryption means for decrypting the key renewal block decryptable using at least one of the node key and the leaf key provided in said information recording device to calculate an encrypting key used in encrypting data to be stored in said recording medium; said encryption means encrypting the data to be stored in said recording medium using the calculated encrypting key;

said encryption means detecting, in encrypting and storing the content for said recording medium, the latest usable key renewal block from key renewal blocks stored in said recording medium and from the key renewal block stored in said memory means of the information recording device itself; said encryption means encrypting the data to be stored on said recording medium using the encrypting key obtained on decrypting the detected latest usable key renewal block.

2. The information recording device according to claim 1 wherein said encrypting key is one of a master key common to the plural information recording devices, a device

key unique to each information recording device and a media key set so as to be unique to each information recording device.

3. The information recording device according to claim 1 wherein said information recording device is configured for executing the processing of writing the latest usable one of the key renewal blocks stored on said recording medium and the key renewal block stored in the memory means of the information recording device itself on the recording medium in case the latest usable key renewal block is the key renewal block stored in the memory means of the information recording device itself and the latest key renewal block is not as yet stored on the recording medium.

4. The information recording device according to claim 1 wherein said information recording device is configured for executing the processing of writing the latest usable one of the key renewal blocks stored on said recording medium and the key renewal block stored in the memory means of the information recording device itself, on the recording medium, in case the latest usable key renewal block is the key renewal block stored in the memory means of the information recording device itself and the latest key renewal block is not as yet stored on the recording medium.

5. The information recording device according to claim 1 wherein said node key is configured as a renewable key and, in a renewal processing of said encrypting key, a key renewal block encrypted using a key including at least a lower layer node key or a lower layer leaf key is distributed to an information recording device as a leaf to be supplied with said encrypting key;

said encryption means in said information recording device receiving the encrypting key encrypted with said renewal node key;

acquiring said renewal node key by encryption processing of said key renewal block; and

calculating said encrypting key based on the acquired renewal node key.

6. The information recording device according to claim 1 wherein said encrypting key is associated with a version number as the generation information.

7. An information reproducing device for reproducing the information from a recording medium, comprising:

memory means for holding a node key unique to each node of a hierarchical tree structure having a plural number of such information reproducing devices operating as leaves, and a leaf key unique to each information reproducing device, said memory means also holding key renewal blocks each formed as renewal key storage data decryptable using at least one of the node key and the leaf key; and

encryption means for decrypting the key renewal block decryptable using at least one of the node key and the leaf key provided in said information reproducing device to calculate an encrypting key used for decrypting the cipher data stored in said recording medium; said encryption means decrypting the cipher data stored in said recording medium using the calculated encryption key;

said encryption means detecting, in the processing of decrypting the cipher data stored in said recording medium, the one of the key renewal block stored in the

recording medium and the key renewal block stored in the memory means of the reproducing device itself, which has a version coincident with the version of the encrypting key of the content to be reproduced; said encryption means executing the decrypting processing of the cipher data stored on the recording medium using the encrypting key obtained by the processing of decrypting the detected key renewal block.

8. The information reproducing device according to claim 7 wherein said encrypting key is one of a master key common to the plural information recording devices, a device key unique to the information recording device and a media key set so as to be unique to each information recording device.

9. The information reproducing device according to claim 7 wherein said information recording device is configured for executing the processing of writing the latest usable one of the key renewal blocks stored on said recording medium and the key renewal block stored in the memory means of the information recording device itself, in the memory means of the recording and/or reproducing device itself, in case the latest usable key renewal block is the key renewal block stored in the recording medium and the latest key renewal block is not as yet stored in the memory means of the recording and/or reproducing device itself.

10. The information reproducing device according to claim 7 wherein said node key is configured as a renewable key and, in a renewal processing of said encrypting key, a key renewal block obtained on encrypting a renewal node key using a key including

at least a lower layer node key or a lower layer leaf key is distributed to an information recording device as a leaf to be supplied with said encrypting key;

said encryption means in said information recording device receiving the encrypting key encrypted with said renewal node key;

acquiring said renewal node key by encryption processing of the key renewal block; and

calculating said encrypting key based on the acquired renewal node key.

11. The information reproducing device according to claim 7 wherein said encrypting key is associated with a version number as the generation information.

12. An information recording method in an information recording device adapted for recording the information for a recording medium, said information recording device holding a node key unique to each node of a hierarchical tree structure having a plural number of such information recording devices, operating as leaves, and a leaf key unique to each information recording device, said method comprising:

a step of detecting the latest usable one of the key renewal blocks stored in the recording medium and the key renewal block stored in said memory means of the information recording device itself;

a step of decrypting the detected latest usable key renewal block, at said detection step, using at least the node key or the leaf key held in said information recording device, to calculate the encrypting key used in encrypting the data stored in said recording medium; and

a step of encrypting the recording data for said recording medium, using the calculated encrypting key, to store the encrypted data on the recording medium.

13. The information recording method according to claim 12 wherein, in case the detected latest usable key renewal block is the key renewal block stored in the memory means of the information recording device itself and the latest key renewal block has as yet not been stored in the recording medium, said detection step executes the processing of writing the latest key renewal block in said recording medium.

14. The information recording method according to claim 12 wherein, in case the detected latest usable key renewal block is the key renewal block stored in the recording medium and the latest key renewal block has as yet not been stored in the memory means of the information recording device itself, said detection step executes the processing of writing the latest key renewal block in said memory means of the information recording device itself.

15. An information reproducing method in an information recording device adapted for recording the information for a recording medium, each of a plurality of such devices holding a node key unique to each node of a hierarchical tree structure having the plural respective information recording devices operating as leaves, and a leaf key unique to each information reproducing device, said method comprising:

a step of acquiring the version information of an encrypting key for the content being reproduced, stored in a recording medium;

a step of detecting the one of the key renewal block stored in the recording

medium and the key renewal block stored in a memory means of the reproducing device itself, which has a version coincident with the version of the encrypting key of the content to be reproduced;

a step of generating an encrypting key by decryption processing of a key renewal block as detected by said detection step; and

a step of decrypting the cipher data stored in the recording medium using the generated encrypting key.

16. The information reproducing method according to claim 15 wherein said detection step executes the processing of writing the latest usable one of the renewal blocks in the memory means of the information recording device itself, in case the latest usable key renewal block is the key renewal block stored in the recording medium and the latest key renewal block is not as yet stored in the memory means of the information recording device itself.

17. An information recording medium capable of recording the information, said recording medium having stored therein, as key renewal blocks having different configurations, a plural number of key renewal blocks, each obtained on encrypting a renewal node key contained in each node key unique to each node forming a hierarchical tree structure having a plural number of information recording or reproducing devices operating as leaves, and a leaf key unique to each information recording or reproducing device, using a key including at least a leaf key or a node key of a lower layer.

18. The information recording medium according to claim 17 wherein said key renewal block is associated with a version number as the generation information.

19. A computer program for executing on a computer system the information recording processing in an information recording device which holds a node key unique to each node forming a hierarchical tree structure having plural such information recording devices, operating as leaves, and a leaf key unique to each information recording device, and which records the information on a recording medium, said program including:

a detecting step of detecting the latest usable key renewal block from the key renewal blocks stored in the recording medium and the key renewal block stored in the memory means of the information recording device itself;

a decrypting step of decrypting the detected latest usable key renewal block at said detecting step using at least one of the node key and the leaf key provided in the information recording device, to calculate the encrypting key used in encrypting the data stored on said recording medium; and

a step of encrypting the recording data for said recording medium using the encrypting key as found in said decrypting step to store the encrypted recording data on the recording medium.

20. A computer program for executing on a computer system the information reproducing processing in a information reproducing device holding a node key unique to each node forming a hierarchical tree structure having the plural such

information reproducing devices operating as leaves, and a leaf key unique to each information reproducing device, and which decrypts the cipher data stored in the recording medium; said program including:

a step of acquiring the version information of an encrypting key of the content to be reproduced, stored on a recording medium;

a step of detecting a key renewal block having a version coincident with the version of the encrypting key of the content to be reproduced, from the key renewal blocks stored in the recording medium and the key renewal block stored in the memory means of the information recording device itself;

a step of generating an encrypting key by decryption processing of the key renewal block detected in said detecting step; and

a step of decrypting the cipher data stored on the recording medium using the generated encrypting key.

21. An information recording device for recording the information on a recording medium, each recording device comprising:

memory means for holding a node key unique to each node of a hierarchical tree structure having a plural number of such information recording devices operating as leaves and a leaf key unique to each information recording device, said memory means also holding a key renewal block each formed as renewal key storage data decryptable using at least one of the node key and the leaf key;

encryption means for decrypting the key renewal block formed as renewal key

storage data decryptable using at least one of the node key and the leaf key provided in said information recording device to calculate an encrypting key used in encrypting the data to be stored in said recording medium; said encryption means encrypting the data stored in said recording medium using the calculated encrypting key; and

renewing means for comparing, in accessing the recording medium, the version of a key renewal block stored in the recording medium to that of the key renewal block owned by the information recording device itself, and for writing the key renewal block of the new version on the recording medium if the key renewal block of the new version is the key renewal block stored in the memory means of the recording device itself, and the key renewal block of the new version is not as yet stored on the recording medium.

22. The information recording device according to claim 21 wherein, if the latest usable one of the key renewal block is the key renewal blocks stored on the recording medium and the latest usable key renewal block has not as yet been recorded in the memory means of the recording device itself, said renewing means writes the latest key renewal block in the memory means of the recording device itself.

23. The information recording device according to claim 21 wherein said renewal processing means detects such a one of the key renewal blocks stored on a recording medium, not used for encrypting any content data stored on said recording medium and which is not the latest one on the recording medium, and deletes the detected key renewal block from the recording medium.

24. The information recording device according to claim 21 wherein, in encryption and storage processing of the content for said recording medium, said encryption means detects the latest usable one of the key renewal blocks stored in the recording medium and the key renewal block stored in the memory means of the information recording device itself and, using the encryption key acquired by decryption processing of the detected latest usable key renewal block, undertakes to encrypt the data to be stored in said recording medium.

25. The information recording device according to claim 21 wherein said encrypting key is one of a master key common to the plural information recording devices, a device key unique to each information recording device and a media key set so as to be unique to each information recording device.

26. The information recording device according to claim 21 wherein said node key is configured as a renewable key and, in renewing the encrypting key, a key renewal block obtained on encrypting a renewal node key by a key at least including one of a node key of a lower layer and a leaf key of a lower layer is distributed to the information recording device of the leaf intended to be furnished with the encrypting key;

said encryption means in said information recording device receiving the encrypting key encrypted using the renewal node key; and

acquiring said renewal node key to calculate said encrypting key based on the acquired renewal node key.

27. The information recording device according to claim 21 wherein said encrypting key is associated with a version number as the generation information.

28. An information reproducing device for reproducing the information from a recording medium, each information reproducing device comprising:

memory means for holding a node key unique to each node of a hierarchical tree structure having a plural number of such information reproducing devices operating as leaves and a leaf key unique to each information reproducing device, said memory means also holding a key renewal blocks formed as renewal key storage data decryptable using at least one of the node key and the leaf key;

encryption means for decrypting the key renewal block decryptable using at least one of the node key and the leaf key provided in each information reproducing device to calculate an encrypting key used in encrypting data to be stored in said recording medium; said encryption means decrypting the data stored in said recording medium, using the calculated encrypting key; and

renewal means for comparing, in accessing the recording medium, the version of a key renewal block stored in the recording medium to that of the key renewal block owned by the reproducing device itself, and for writing the key renewal block of the new version in the recording medium, if the key renewal block of the new version is the key renewal block stored in the memory means of reproducing device itself, and the key renewal block of the new version is not as yet stored on the recording medium.

29. The information reproducing device according to claim 28 wherein, if the latest

usable one of the key renewal blocks stored on the recording medium and the key renewal block owned by the information reproduced device itself is the key renewal block stored on the recording medium, and said latest key renewal block has as yet not been stored in the memory means of the information recording device itself, said renewing means writes said latest key renewal block in the memory means of the information reproducing device itself.

30. The information reproducing devices according to claim 28 wherein said renewal means detects such a one of the key renewal blocks stored in the recording medium, not used in encrypting any of content data stored on said recording medium and which is not the latest one on the recording medium, and deletes the detected key renewal block from the recording medium.

31. The information reproducing devices according to claim 28 wherein said encryption means detects, in the processing of decrypting the cipher data stored in said recording medium, the one of the key renewal blocks which is stored in the recording medium and the key renewal block stored in the recording and/or reproducing device itself, and which has a version coincident with the version of the encrypting key of the content to be reproduced; said encryption means executing the decrypting processing of the cipher data stored on the recording medium using the encrypting key obtained by the processing of decrypting the detected key renewal block.

32. The information reproducing devices according to claim 28 wherein said encrypting key is one of a master key common to the plural information recording

devices, a device key unique to each information recording device and a media key set so as to be unique to each information recording device.

33. The information reproducing device according to claim 28 wherein said node key is configured as a renewable key and, in renewing the encrypting key, a key renewal block obtained on encrypting a renewal node key by a key at least including one of a node key of a lower layer and a leaf key of a lower layer is distributed to an information recording device of the leaf intended to be furnished with the encrypting key;

said encryption means in said information recording device receiving the encrypting key encrypted using the renewal node key and acquiring said renewal node key by encrypting the key renewal block to calculate said encrypting key based on the acquired renewal node key.

34. The information reproducing device according to claim 28 wherein said encrypting key is associated with a version number as the generation information.

35. In a recording or reproducing device including a node key unique to each node forming a hierarchical tree structure having a plural number of such information recording devices, operating as leaves, and a leaf key unique to each recording device, said device being adapted for recording the information on a recording medium, a method for renewing an encrypting key comprising:

a detection step of detecting the latest usable one of the key renewal blocks stored on the recording medium and the key renewal block stored in the memory

means of the recording or reproducing device; and

a renewal step of undertaking, in case the latest version of the key renewal block is the key renewal block stored in the memory means of the information recording or reproducing device itself and the key renewal block of the new version has not been stored on the recording medium, the writing of said key renewal block of the new version on said recording medium.

36. The encrypting key renewing method according to claim 35 wherein said renewing step further includes a step of undertaking, in case the latest usable one of the key renewal blocks stored on said recording medium and the key renewal block owned by the information recording or reproducing device itself is the key renewal block stored on said recording medium, and the latest key renewal block has as yet not been stored in the memory means of the information recording or reproducing device, the processing of writing said latest key renewal block in the memory means of the recording and/or reproducing device itself .

37. The encrypting key renewing method according to claim 35 wherein said renewing step further includes a step of detecting such a one of the key renewal blocks stored in the recording medium, not used in detecting any content data stored on said recording medium and which is not the latest key renewal block on the recording medium, said renewing step also deleting the detected key renewal block from the recording medium.

38. A computer program for having a computer system execute encryption key

renewal processing in an information recording or reproducing device for recording or reproducing the information for a recording medium, holding a node key unique to each node forming a hierarchical tree structure having a plural number of information recording devices operating as leaves, and a leaf key unique to each information recording device, said computer program including:

a detection step of detecting the latest usable key renewal block of the new version of the key renewal blocks stored on the recording medium and the key renewal block stored in the memory means of the recording or reproducing device itself; and

a renewal step of undertaking, in case the latest version of the key renewal block is the key renewal block stored in a memory means of the information recording or reproducing device itself and the key renewal block of the new version has not been stored on the recording medium, the writing of said key renewal block of the new version on said recording medium.